

AMENDMENTS TO THE CLAIMS

The following is a complete, marked-up listing of revised claims with a status identifier in parenthesis, underlined text indicating insertions, and strike through and/or double-bracketed text indicating deletions.

LISTING OF CLAIMS

1. (Currently Amended) A pairing control method between a first device and a second device, the pairing control method aiming to secure the data exchange with the aid of a unique pairing key, the pairing control method comprising:

- verifying the pairing between the two devices and using the unique pairing key ~~[[if]]~~when the pairing between the two devices has been already carried out, wherein, when the paring between the two devices has not been carried out, the method includes~~if not,~~

- searching for a free location among the locations reserved for the unique pairing key~~pairing data~~ in the first device and wherein, when a free location is absent, the method further includes performing at least one of

- reading an activity counter associated with each location of the first device, said activity counter being incremented each time a location is used for pairing, and finding a lowest value activity counter to determine the location to be used for a pairing procedure, and

- reading a chronology counter associated with each location of the first device, said chronology counter being incremented each time a location is used for pairing, and finding a lowest value chronology counter to determine the location to be used for a pairing procedure~~in this case,~~

- initiating ~~[[a]]~~the pairing procedure by transmitting a cryptogram contained in the second device, the cryptogram including an identifier ~~belonging to~~ identifying

the second device and the unique pairing key, and the cryptogram being encrypted by a secret key common to all the first devices,

- decrypting the cryptogram with the first device and extracting the identifier of the second device and the unique pairing key from the cryptogram, and
- storing the unique pairing key in the first device, the unique pairing key used to pair with the second device.

2. (Previously Presented) The method according to claim 1, wherein the unique pairing key is based on the identifier of the second device and on the data of the first device.

3. (Previously Presented) The method according to claim 1, wherein the cryptogram is stored in the first device and encrypted with a secret key common to a plurality of second devices.

4. (Cancelled)

5. (Previously Presented) The method according to claim 1, wherein pairing is conditioned by the introduction of a secret code transmitted to the first device and verified by said first device.

6. (Previously Presented) The method according to claim 5, wherein the secret code belongs to and is unique to each first device.

7. (Previously Presented) The method according to claim 5, wherein the required secret code is different in each pairing.

8. (Currently Amended) The method according to claim 5 further comprising:

- transmitting a unique identifier of the first device and ~~a unique~~ the identifier of the second device to a management centre,

- verifying the conformity of ~~this~~ the pairing and calculating, by means of the management centre, ~~a~~ the corresponding secret code on the basis of the two identifiers,

- transmitting ~~this~~ the secret code to ~~the~~ a user,

- initiating the pairing and requesting the introduction of the secret code, by means of the first device,

- calculating by means of the first device the necessary secret code on the basis of the identifiers of the first and second devices,

- comparing the calculated code with ~~that which has been~~ a code introduced by the user,

- accepting the pairing if the two codes are identical.

9. (Previously Presented) The method according to claim 8 further comprising, determining the new secret code on the basis of the two identifiers and of an index that represents the number of pairings previously carried out, whereas the first device stores this index in its memory.

*** END CLAIM LISTING **